

Ser. No. 09/817,324

01P04786US

REMARKS

Claims 1-4, 6, 9, 11, 14, 19, 21 and 23 are amended to correct formality errors identified in the Rejection and to more clearly recite the invention.

Claim 2 is amended to be in independent form including the limitations of the original base claim, claim 1.

Support for the amendments is found in the existing claims and in the Application description in connection with Figure 2 and other places. Specifically, support for "communicating application specific context information in a data field of a URL separately from session identification information" is found in the Application on page 5 lines 25-37 and lines 31-33. This section indicates "Manager 250 employs a system protocol for passing session context information to applications 200 and 230 via URL query or form data. The session context information comprises a session identifier, a hash value, and application specific data. Support for the "application specific context information supporting acquisition from said second application of information associated with a current operational context of said first application" is found in the existing claims and in the Application, e.g., "The application specific data is tailored to meet the intended function of a target application" on page 5 lines 33-35 and in other places.

I. Claim objections.

Claims 2 and 9 are objected to because of informalities. Specifically, claim 2 is objected to because of a comma after the term "incorporates" and claim 9 is objected to because of a comma after the term "portion".

These commas have been deleted in claims 2 and 9 in accordance with the Examiners suggestion. Consequently, the objection to claims 2 and 9 is believed to be satisfied and its withdrawal is respectfully requested.

II. Rejection of claims 2-5, 9 and 11 under 35 USC 112.

Claims 2-5, 9 and 11 are rejected under 35 USC 112 second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter. Specifically, claims 2-4, 9 and 11 are rejected in that it is unclear which processor in the recited term "said at least one communication processor" is referred

Ser. No. 09/817,324

01P04786US

to by the term "said communication processor".

Claims 2-4, 9 and 11 are amended to recite "a communication processor of said at least one communication processor". As such this term unambiguously recites the term "a communication processor" of "said at least one communication processor". Therefore any "processor" of "said at least one communication processor" may perform the function recited in claims 2-4, 9 and 11. Claim 5 is rejected based on its dependence on claim 4. Consequently, claims 2-5, 9 and 11 are no longer unclear and withdrawal of this rejection is respectfully requested.

III. Rejection under 35 U.S.C. 103(a)

Claims 1-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,178,511 – Cohen et al in view of U.S. Patent 5,708,780 – Levergood et al.. These claims are considered patentable for the following reasons.

Claim 1 recites a system "used by a first application for managing user access to at least one of a plurality of network compatible applications" comprising "an authentication processor for, receiving user identification information including a user identifier and initiating authentication of said user identification information using an authentication service; and at least one communication processor for, communicating an authentication service identifier and a corresponding user identifier to a managing application, said authentication service identifier identifying an authentication service used to authenticate identification information of said corresponding user and automatically communicating application specific context information in a data field of a URL separately from session identification information, to a second application of said plurality of network compatible applications in response to a user command to initiate execution of said second application and in response to authentication of said user identification information, said application specific context information supporting acquisition from said second application of information associated with a current operational context of said first application". These features are not shown or suggested in Cohen with Levergood either individually or in combination.

The system of amended claim 1 includes "automatically communicating application specific context information in a data field of a URL separately from session identification information, to a second application of said plurality of network compatible applications in response to a user command to initiate

Ser. No. 09/817,324

01P04786US

execution of said second application and in response to authentication of said user identification information". Such application specific context information includes a patient identifier or user identifier, for example (Application page 10 lines 35-37). The claimed system advantageously "automatically" communicates "application specific context information in a data field of a URL separately from session identification information, to a second application of said plurality of network compatible applications" such as a patient identifier "in response to authentication of said user identification information" initiated by the "authentication processor". Further, the "application specific context information" supports "acquisition" from the "second application of information associated with a current operational context of said first application".

Thereby the system enables a user to logon and authenticate with a first application such a patient census application and gain automatic access to multiple other applications such as a medical laboratory test result application and in response to user authentication with the test result application, be automatically provided with desired test results for the specific patient selected in the first patient administration application (see example described on Application page 5 lines 8-12 and elsewhere in connection with Figure 2). This is done without the user having to re-enter context information (e.g., a patient identifier) by link selection or another command following automatic authentication with a second application. This capability is not shown or suggested in Cohen with Levergood. The combination of automatic authentication to multiple applications together with automatic communication of application specific context information "in response to a user command to initiate execution of said second application and in response to authentication of said user identification information" facilitates user friendly operation and user seamless navigation in a plurality of concurrently operating applications. The system addresses the problems involved in "facilitating user initiation (e.g., logon), operation and termination (e.g., logoff) of multiple Internet applications and in securely passing URL, patient (and user) identification and other information between applications. A managing application is employed to coordinate user operation sessions. Specifically the managing application coordinates inactivity timeout operation and maintains and conveys properties between concurrent applications in order to create a smooth user operation session" (Application page 4 lines 23-31).

The Rejection on page 4 recognizes that Cohen does not disclose "automatically" communicating "application specific context information" in "a data field of a URL" to a "second application of said plurality of network compatible

Ser. No. 09/817,324

01P04786US

applications" in "response to authentication of said user identification information" initiated by the "authentication processor". However, Levergood (with Cohen) in column 4 lines 1-18 relied on in the Rejection on page 4 also fails to show or suggest "automatically" communicating "application specific context information" (such as a patient identifier) in "a data field of a URL" to a "second application of said plurality of network compatible applications" in "response to authentication of said user identification information" initiated by the "authentication processor". Cohen does not mention, contemplate or suggest Internet based operation and communication of data via URL data fields.

Levergood in column 4 lines 1-18 or elsewhere nowhere mentions "application specific context information" or context information at all. Levergood discusses a browser that rewrites a URL link to include new Session Identification Information (SID) in response to a user electing to traverse a link (Levergood column 4 lines 7-10) and rewrites a URL to include a new SID but "the new URL retains all portions of the old, including the SID, except for the new page name" (Levergood Column 3 lines 64-65). Levergood also redirects a URL, specifically an "authentication server then forwards a new request consisting of the original URL appended by the SID to the client in a REDIRECT" (column 3 lines 37-41). Nowhere however does Levergood mention, show or suggest "automatically" communicating "application specific context information" (such as a patient identifier) in "a data field of a URL separately from session identification information," to a "second application of said plurality of network compatible applications" in "response to authentication of said user identification information" initiated by the "authentication processor". Levergood discloses appending session identification information (SID) to a URL (column 3 line 39), however session identification is used for authentication and determining access to documents (a user is provided with a session identification which allows the user to access to the requested file as well as any other files within the present protection domain" - Levergood Abstract). Session identification information is not "application specific context information" and does NOT support "acquisition from said second application of information associated with a current operational context of said first application".

Levergood (with Cohen) does not show or suggest "automatically" communicating "application specific context information" (such as a patient identifier) in "a data field of a URL separately from session identification information". Cohen with Levergood also does not suggest these features in combination with facilitating automatic authentication to multiple network

Ser. No. 09/817,324

01P04786US

compatible applications" by "communicating an authentication service identifier" and a "corresponding user identifier to a managing application". Consequently withdrawal of the Rejection of amended claim 1 under 35 USC 103(a) is respectfully requested.

Amended independent claim 2 recites a system "used by a first application for managing user access to at least one of a plurality of network compatible applications" comprising "an authentication processor for, receiving user identification information including a user identifier and initiating authentication of said user identification information using an authentication service; and at least one communication processor for, communicating an authentication service identifier and a corresponding user identifier to a managing application, said authentication service identifier identifying an authentication service used to authenticate identification information of said corresponding user and automatically communicating application specific context information in a data field of a URL to a second application of said plurality of network compatible applications in response to a user command to initiate execution of said second application and in response to authentication of said user identification information wherein said application specific context information comprises at least one of, (a) a user identifier and (b) a patient identifier and a communication processor of said at least one communication processor encrypts an address portion of said URL and incorporates said encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form, into a single processed URL data string". These features are not shown or suggested in Cohen with Levergood.

Amended independent claim 2 is considered to be patentable for reasons given in connection with claim 1 and for the following reasons. Cohen with Levergood does NOT discuss or suggest "automatically" communicating "application specific context information in a data field of a URL" such as a patient identifier" to a "second application of said plurality of network compatible applications" in "response to authentication of said user identification information" in combination with facilitating automatic authentication to multiple network compatible applications" by "communicating an authentication service identifier" and a "corresponding user identifier to a managing application". Cohen with Levergood also fails to show or suggest encrypting an "address portion of said URL link" to the "second application" and incorporating the "encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form, into a single processed URL data string". In an exemplary embodiment of the invention illustrated in the

Ser. No. 09/817,324

01P04786US

Application specification pages 11-12, application 200 advantageously, for example, encrypts "a URL link address portion" comprising a hash value identified by field identifier GSH= derived by "hashing on the addressable portion of a fully qualified URL" comprising the "URL data either lying between the "http://" and the question mark "?" or from the data lying between the "http://" and the pound/number sign "#" - whichever comes first" (Application page 9 lines 31-33 and page 11 line 25). Consequently, in the exemplary URL string shown processed in the specification page 12

www.smed.com/altoona/prd/results.exe/1?GSM=16253384937&GSH=24017
&Pid=1772693&Frgclr=blue

the compressed address portion is 24017 which is concatenated with a patient identifier (Application page 12 line lines 15-20) as shown:

GSH=24017&Pid=1772693

and is encrypted into the string

16sfdjwhejeyw7rh3hekw

to produce the processed URL including the encrypted URL address portion:

www.smed.com/altoona/prd/results.exe/1?GSM=16253384937:16sfdjwhejey
w7rh3hekw&Frgclr=blue.

This is an exemplary "processed URL". The Rejection makes a fundamental error on page 5 in interpreting the Levergood reference. Contrary to the Rejection statements on page 5, Levergood in column 4 line 64 to column 5 line 2, column 5 lines 56-65 and column 3 lines 34-37 relied on in the Rejection merely discloses encryption of a session identifier (SID) and an IP address. Specifically, Levergood states "the digital signature is a cryptographic hash of the remaining items in the SID and the authorized IP address which are encrypted with a secret key which is shared by the authentication and content servers"- Levergood column 5 lines 61-65, also see column 3 lines 33-37).

Further, although in Levergood a valid session identifier "typically comprises" an "accessible domain" in the "SID encrypted with a secret key", the

Scr. No. 09/817,324

01P04786US

Levergood accessible domain is NOT a URL or an address portion of a URL (Levergood column 3 lines 33-37). Levergood explicitly defines an accessible "domain" as a collection of files and NOT a URL or address portion of a URL ("A protection domain is defined by the service provider and is a collection of controlled files of common protection within one or more servers" – Levergood column 3 lines 52-55). This is further made clear in column 5 lines 54-61 stating a "preferred SID is a sixteen character ASCII string that encodes 96 bits of SID data" that contains "an 8-bit domain comprising a set of information files to which the current SID authorizes access". Such an "accessible domain" as used by Levergood is not in a URL link address portion. This is further corroborated in Levergood in column 6 lines 29-34 indicating that such a domain is in the non-address, URL data field portion of a URL (e.g. after the question mark), specifically, a "REDIRECT URL might be: "http://auth.com/authenticate?domain= [domain]& URL = http://content.com/report".

Levergood does not show or suggest encrypting an "address portion of said URL link" to the "second application" and incorporating the "encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form, into a single processed URL data string". Neither a session identifier nor an IP address as used in Levergood are a "URL or a URL address portion". Indeed a URL and IP address are distinct and different objects with totally different functions ("the content server records the URL and the IP address" – Levergood column 5 lines 37-38). An IP address describes an electronic address of an Internet entity whereas a URL "consists of three parts: the transfer format, the host name of the machine that holds the file, and the path to the file" (Levergood column 2 lines 28-31). A session identifier identifies a user session of computer operation for example and is itself a distinct entity that may be conveyed within a field of a URL (Application page 11 line 17).

The purpose of the Levergood encryption is to ensure validity of session identifiers (SIDs) by using an "Internet server" to subject "the client to an authorization routine prior to issuing the SID" (Levergood column 3 lines 24-26). In contrast, the Application addresses the problem of preventing "URL replay or redirection" through its recognition that URLs are "vulnerable to corruption" (Application page 11 lines 1-9). Consequently there is no reason, problem recognition or motivation for amending the Levergood system to include the claimed arrangement. Consequently, withdrawal of the rejection of claim 2 under 35 USC 103(a) is respectfully requested.

Ser. No. 09/817,324

01P04786US

Amended dependent claim 3 is considered to be patentable based on its dependence on claim 1. Claim 3 is also considered to be patentable because Cohen with Levergood does not show or suggest a system in which "said application specific context information comprises a patient identifier, a communication processor of said at least one communication processor also communicates a session identifier identifying a user initiated session of operation of said first application to said managing application and said user identification information includes a password associated with said user identifier". As previously explained in connection with claim 1, Cohen with Levergood does not suggest "automatically" communicating "application specific context information" comprising "a patient identifier" in "a data field of a URL separately from session identification information".

Amended dependent claim 4 is considered to be patentable based on its dependence on claim 1. Claim 4 is also considered to be patentable because Cohen with Levergood does not show or suggest a system in which "a communication processor of said at least one communication processor communicates said authentication service identifier and said corresponding user identifier to a managing application for compilation of a database". Contrary to the Rejection statement on page 5, Cohen in Column 4 line 61 to column 5 line 6, lines 16-22 and 45-58 does not suggest "compilation of a database" including "authentication service identifier and said corresponding user identifier" data pairs. Cohen with Levergood column 4 line 61 to column 5 line 6 recites "Preferably, PKM 24 is a secure, globally accessible repository that facilitates the single sign-on process. Although not meant to be limiting, with respect to a given user, the PKM (as will be described) preferably stores such information as a *username, a set of one or more password(s), and any other application environment-specific information such as domain name, hostname, application name, and the like*. Because this access information preferably is centralized in the PKM, users can access their target resources with one sign-on from any workstation. They can also manage their passwords from this one repository, as will also be seen". It is well understood that citation of a general list of items such as those italicized fail to provide 35 USC 112 compliant enabling disclosure of specific elements such as the recited "authentication service identifier and said corresponding user identifier" data pairs. Further, Cohen with Levergood fails to show or suggest communicating "said authentication service identifier and said corresponding user identifier to a managing application for compilation of a database". In Cohen with Levergood there is no suggestion of dynamic "compilation" of a database. There is no indication in Cohen with Levergood of HOW the PKM repository is provided or any indication other than it is predefined.

Ser. No. 09/817,324

01P04786US

Dependent claim 5 is considered to be patentable based on its dependence on claims 1 and 4. Claim 5 is also considered to be patentable because Cohen with Levergood does not show or suggest a feature combination as in claim 5 involving a database "accessible by other applications of said plurality of network compatible applications for mapping a non-authenticated user identifier of a participant application to an authenticated and different user identifier of another application".

Amended independent claim 6 recites a "system used for processing user access to network compatible applications" comprising "an authentication processor for, receiving authentication service identifier and corresponding user identifier data pairs from at least one of a plurality of applications, compiling a database using said data pairs, mapping a non-authenticated user identifier of a second application to an authenticated different user identifier of a first application using said database; and at least one communication processor for, communicating said authenticated different user identifier to said second application and automatically communicating application specific context information in a data field of a URL separately from session identification information, to said second application in response to a user command to initiate execution of said second application, said application specific context information supporting acquisition from said second application of information associated with a current operational context of said first application".

Amended independent claim 6 is considered to be patentable for the reasons given in connection with claims 1, 4 and 5. Claim 6 is also considered to be patentable because Cohen with Levergood does not show (or suggest) a feature combination as in claim 6 including "compiling a database" using "data pairs, mapping a non-authenticated user identifier of a second application to an authenticated different user identifier of a first application using said database" and at least one communication processor for, "automatically communicating application specific context information in a data field of a URL separately from session identification information, to said second application in response to a user command to initiate execution of said second application". Cohen with Levergood does not show or suggest "compilation of such a database" in combination with automatically communicating application specific context information in a data field of a URL separately from session identification information, to said second application in response to a user command to initiate execution of said second application". Cohen

Ser. No. 09/817,324

01P04786US

with Levergood also does not mention, contemplate or suggest "automatically communicating" "application specific context information supporting acquisition from said second application of information associated with a **current** operational context of said **first application**".

Dependent claim 7 is considered to be patentable based on its dependence on claim 6. Claim 7 is also considered to be patentable because Cohen with Levergood does not show or suggest the feature combination of claim 7 in which "said authentication service identifier identifies an authentication service used to authenticate identification information comprising a user identifier of said corresponding user to provide an authenticated user identifier". Cohen's mention of "information on how to logon to the applications configured on a given machine" in column 4 lines 48-50 fails to provide 35 USC 112 compliant enabling disclosure of an "authentication service identifier" that "identifies an authentication service used to authenticate identification information comprising a user identifier of said corresponding user to provide an authenticated user identifier" in combination with the other features of this claim.

Dependent claim 8 is considered to be patentable based on its dependence on claim 6. Claim 8 is also considered to be patentable because Cohen with Levergood does not show or suggest the feature combination of claim 8 in which "said authentication processor performs said mapping using said database by matching an authentication service identifier of said second application with an authentication service identifier of said first application and providing said authenticated different user identifier of said first application as a mapped user identifier". Cohen column 6 lines 26-37 relied on in the Rejection on page 6 fails to provide 35 USC 112 compliant enabling disclosure of an "authentication processor" that "performs said **mapping** using said database by matching an authentication service identifier of said second application with an authentication service identifier of said first application and providing said **authenticated different user identifier** of said first application as a **mapped user identifier**". These features are not specifically shown or suggested in Cohen with Levergood.

Amended dependent claim 9 is considered to be patentable based on its dependence on claim 6. Claim 9 is also considered to be patentable because of reasons given in connection with claim 2.

Ser. No. 09/817,324

01P04786US

Dependent claim 10 is considered to be patentable based on its dependence on claim 6.

Amended dependent claim 11 is considered to be patentable based on its dependence on claim 6. Claim 11 is also considered to be patentable because Cohen with Levergood does not show or suggest the feature combination of claim 11 in which "a communication processor of said at least one communication processor communicates a parameter to said second application, said parameter identifying success or failure of said mapping". The Rejection alleges this feature is shown in Cohen and relies for support on column 10 lines 35-37 ("Return codes from the interface are associated with buckets (rc.. success, rc_error, etc.), allowing the appropriate action to be taken based on the bucket into which the return code falls"). However, "Return codes... allowing the appropriate action to be taken based on the bucket into which the return code falls" does not show or suggest (or provide a 35 USC 112 enabling disclosure of) communicating "a parameter to said second application...identifying success or failure of". "mapping a non-authenticated user identifier of a second application to an authenticated different user identifier of a first application using" a compiled "database". As previously explained Cohen with Levergood does not discuss dynamic "compilation" of such a database at all.

Dependent claims 12 and 13 are considered to be patentable based on their dependence on claim 6.

Amended independent claim 14 recites a "system used for processing user access to Internet compatible applications," comprising "an authentication processor for, receiving an authentication service identifier and corresponding user identifier from a parent application, and mapping a non-authenticated user identifier of a child application to an authenticated different user identifier of said parent application; and at least one communication processor for, communicating said authenticated different user identifier to said child application and automatically communicating application specific context information in a data field of a URL separately from session identification information, to said child application in response to a user command to initiate execution of said child application and in response to communicating said authenticated different user identifier, said application specific context information supporting acquisition from said child application of information associated with a current operational context of said parent application". Amended independent claim 14 is considered to be patentable for the reasons given in connection with claims 1, 4, 5 and 6.

Ser. No. 09/817,324

01P04786US

Dependent claim 15 is considered to be patentable based on its dependence on claim 14.

Dependent claims 16-20 are considered to be patentable based on their dependence on claim 14 and any intervening claim and because of the additional feature combinations they represent for the reasons given in connection with previous claims.

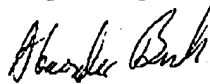
Amended independent method claim 21 mirrors apparatus claim 14 and is considered to be patentable for similar reasons.

Dependent claim 22 is considered to be patentable based on its dependence on claim 21 for reasons given in connection with claim 6.

Amended independent method claim 23 mirrors apparatus claim 1 and is considered to be patentable for similar reasons. Consequently withdrawal of the Rejection of claims 1 - 23 under 35 USC 103(a) is respectfully requested.

In view of the above amendments and remarks, Applicants submit that the Application is in condition for allowance, and favorable reconsideration is requested.

Respectfully submitted,



Alexander J. Burke
Reg. No. 40,425

Date: June 15, 2005

Alexander J. Burke
Customer No. 28524
Tel. 732 321 3023
Fax 732 321 3030